448 Final

Study online at https://quizlet.com/_as14qf

1.	**The goal of stuxnet was to find ____**	a computer used to program a programmable logic computer
2.	**Tool John**	Cracks password through dictionary or brute force, can go off of wordlists
3.	**Tool Hashcat**	Crack hashes of passwords to obtain password text
4.	**Tool Steghide**	Finds hidden files in images
5.	**Tool Splunk**	Used for log viewing
6.	**Tool Wireshark**	Used for viewing network packets
7.	**Tool Zenmap**	Used for banner grabbing and network mapping
8.	**Tool telnet**	Used for banner grabbing, finding whats used on network
9.	**Tool Metasploit**	Finds open ports and sees what they do
10.	**Tool Burp Suite**	SQL injection tool and modification
11.	**Ghidra**	

		Software reverse engineering
12.	**Tool Openvas**	Scans and reports vulnerabilities on web servers
13.	**Tool Armitage**	Finds backdoors and attacks
14.	**Tool Truecrypt Truecrack**	Used for cracking and creating secured partitions
15.	**Tool Ettercap**	man in the middle
16.	**Tool Driftnet**	TCP stream images
17.	**An IPv4 address is comprised of _ bits**	32
18.	**Which of the following is true about symmetric multiporcessing**	A Single copy of the OS is in charge of all the processors The processors share memory and the I/O Bus
19.	**Random and unreadable text messages are called:**	Ciphertext
20.	**With a Kerberos system does the user's password ever get passed across the network?**	No, the users password is stored in the KDC. The users password is authenticated when the KDC uses the password to decrypt the authen-

		ticator which was encrypted by the user with their password
21.	**What are the three parts of the information security triad**	CIA confidentiality, integrity, avaiblitily
22.	**Several programs can be running within the computer, each taking turns using the processor**	Multi tasking
23.	**What type of error is false reject rate**	Type 1 error
24.	**The Zachman framework**	Includes specification for defining and capturing and architecture
25.	**What is the name of the not for profit worldwide charitable organization focused on improving the security of application software that we discussed in class**	Open Web Application Security Project
26.	**Which type of memory outputs on both the rising and falling edges of the clock cycle**	DDR SDRAM
27.	**Which of the following is NOT true about asymmetric cryptography systems**	Faster than symmetric cryptography
28.	**What type of cipher do you think was used to create iihhgph**	Substitution
29.	**What is the most widely accepted approach to IT service management in the world**	ITIL
30.	**The question to ask when making a secuirty decision is**	is it worth the tradeoff
31.	**What type of cipher will produce the exact same cipher text no matter how large the clear text is**	hash

32.	**1) Bob writes the message** **2) Bob encrypts the message with [a]'s [b] key** **3) Bob sends the encrypted message to Alice** **4) Using [c]'s [d] key Alice decrypts the message**	Bob Private Bob Public
33.	**According to Bruce Schreiner, al of the following are biases in risk perception except one**	real-world risks hold more value than online risks
34.	**TLS uses port # ---- when encrypting http**	443
35.	**Decrypt which was encrypted with a ceaser cipher shift of +3**	jump
36.	**Which technology allows users to sign on to a omputer or network once and have theri identification and authoraization credentials allw them intoa ll computers and systems where they are authorized**	SSO Single Sign on
37.	**in order to bring down isis the US needed to hack ___ main accounts**	ten
38.	**What is the vulnerability associated with CPU states**	When a system crashes, there is a core dump of its internal state. If the core dump is not secured then unauthorized users coulda access it
39.	**A certificate authority is**	A trusted third part that associates an identified signer with a specific public key
40.	**THE ITIL framework is broken down into two main groups**	1. Problem Analysis

		2. Design Evaluation
41.	**What type of cryptosystem is a Caesar cipher**	symmetric
42.	**Which of the following is the correct description of DES**	DES encryption employs a symmetric key using a block cipher and 56-bit key for encryption
43.	**One of the security challenges that the task force had to crack was**	"what is the name of your pet?"
44.	**If the network portion of an IP address is the first three octets (10.12.1.x), then the slash notation (also known as CIDR notation) to scan this network is: 10.0.0.0/___**	16
45.	**Put the Waterfall Model stages in the correct order.**	1. Requirements 2. Design 3. Implementation 4. Verification 5. Maintenance
46.	**Place the pieces of an information system in the correct order, starting with the highest level (the part that the end-user directly interacts with is #1).**	1. application program 2. utilities 3. operating system 4. computer hard-

		ware (memory and CPU)
47.	**Decrypt the following message which was encrypted using the vigenere cipher using the passphrase ncl: fwxzgc**	summer (NCL on top then go to passphrase letter, final letter is on left)
48.	**What type of cipher rearranges the characters in the plaintext to form the ciphertext?**	Transposition
49.	**Which of the following identifies the stages of the three-way handshake?**	SYN, SYN/ACK, ACK
50.	**What is the name of the"big idea" to obscure the relationship between your real message and the encrypted message?**	confusion
51.	**The main target of Stuxnet was:**	Natanz nuclear facility
52.	**Access should be granted on a _______ privilege basis.**	least
53.	**What is the following an example of? "All authorized users must be allowed to do only their authorized tasks. Unauthorizedusers must not have access to the company systems or resources."**	Policy
54.	**Policy does NOT include:**	list of technologies to use
55.	**Ping uses the ____ protocol.**	ICMP
56.	**Why is the operation to hack ISIS being talked about publicly?**	American offensive cyber operations only works as a deterrent if

		people know it exists
57.	**A fixed-length value used as a message fingerprint is called a:**	Hash value
58.	**In a Kerberos system, the client first authenticates with the KDC. Then when it requests access to a particular resource what must it present?**	Ticket Granting Ticket (TGT)
59.	**A username and password combination is which type of authentication?**	Single-factor
60.	**Which algorithm did NIST choose to become the Advanced Encryption Standard (AES) replacing DES?**	Rijndael
61.	**What type of error is false accept rate?**	Type II error
62.	**Annualized Rate Of Occurrence. If you have determined that a fire could occur once in ten years and you will lose 50% of your $500,000 asset then your ARO =**	.1
63.	**Which of the following is true about Massively parallel processing? Select all that apply.**	Data paths allow messages to be sent between the processors Can have its own memory (not usually own OS)
64.	**What technology solution blocks attempted attacks to internal web servers?**	WAF
65.	**Confidentiality** **Integrity** **avaiblitly**	eavesdropping and data theft data corruption and tampering service denial and data loss

66.	**"The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it." What part of the security triad does this quote violate?**	availability
67.	**The name of the mission was called _________ ___________ _____________**	Operation Glowing Symphony
68.	**Which of the following lists the correct five levels of the Capability Maturity Model?**	d. Initial, Repeatable, Defined, Managed, Optimizing
69.	**According to the lecture TCO stands for:**	Total cost of ownership
70.	**Which of the following characters would you consider an escape character used for SQL injection (mark all that apply)**	= (equals) -- (dash, dash) ' (single quote) ; (semicolon)
71.	**What is the central repository for all configuration items?**	CMDB
72.	**The second phase of the attack was PSYOP, or driving the adversary crazy. Select everything that they did.**	drained the battery of their cellphone inserted random pictures into videos slowed down the network
73.	**The OWASP website**	ranks the top ten web application vulnerabilities
74.	**Put the following items in the correct order for the flow of an incident on the ITIL service support side:**	1. Service desk

		2. Incident management 3. Change management 4. Release management
75.	**What type of model dictates that all software developers follow a software programming model that uses discrete phases and reviews before the next phase of development is carried out?**	Waterfall
76.	**How did Mikko truck down the Russian punk?**	Mikko discovered the city that the Russian hacker was in based upon the license plate of the car that the hacker posted on social media.
77.	**Which of the following are private IP addresses? (select all that apply)**	172.16.2.1 10.12.3.4 73.48.92.16 192.168.42.42
78.	**Qualitative**	does not attempt to assign numeric value, but is scenario oriented attempts to assign independently objective numeric value to all elements of the risk analysis

79.	**How long has SQL Injection been the top vulnerability?**	It has been the top vulnerability for at least the last decade
80.	**Which of the following are true about a DDOS attack:**	Software is not installed on the site being attacked. The attacker is not after data stored on the site (credit card numbers, SSNs, etc) Involves a botnet which sends a lot of traffic to the victim site.
81.	**What type of error is: false accpetance + false rejection**	crossover error
82.	**According to Johnny Long, how do you "suck data off machines with your mind?"**	shoulder surf
83.	**When you buy insurance you are:**	transferring the risk
84.	**Three methods of authentication are presenting something:**	you know you have you are
85.	**What vulnerability occurs when one process passes pointers to parameters to the OS at the same time another process modifies the parameters?**	TOC/TOU
86.	**According to the lecture BCP stands for:**	Business continuity plan
87.	**What "high tech" instrument did people use to break into phone systems?**	Captain Crunch Whistle

88.	**You would use the following software development model when detailed requirements specification cannot be formulated in advance**	d. Exploratory programming
89.	**The following steps are taken to ensure that a file that the recipient received was not tampered with (it is the original file sent by the sender).**	the file is hashed by the sender the hash is encrypted with the sender's private key and sent to the recipient the recipient hashes the file the recipient decrypts the sender's hash with the sender's public key the recipient compares the decrypted hash with their own hash of the file
90.	**What "acts as filters between us and reality"?**	cognitive biases
91.	**In order to verify the identity of the sender and provide confidentiality you would:**	encrypt first using the sender's private key encrypt again using the receiver's public key
92.	**How do you string two SQL injection queries together?**	You would end the first SQL statement with a closing quote (if needed) , then a semicolon (to denote

		the end of the first query), then the second query with its ending semicolon, and finally a -- for the comment.
93.	**Which of the following is any weakness in a system that makes it possible for a threat to cause it harm?**	Vulnerability
94.	**What does the joke "one, two, three, many" refer to?**	We are all really good at small numbers
95.	**Which technique to control the use of the system's resources is described as:** **The ability of an operating system to execute different parts of a program simultaneously.**	Multithreading
96.	**Which statement is true regarding digital signatures?**	b. Authentication is assured because the sender's private key is used to encrypt the message.
97.	**A standard:**	c. identifies a specific product or mechanism for universal company use
98.	**What type of cipher do you think was used to create the following ciphertext:**	Transposition
99.	**Granting of access privileges to certain files is:**	Authorization
100.		Baselines

	________ are helpful when configuring new computers or devices as well as for comparing with existing systems to see if they still meet the minimums.	
101.	**What technology solution blocks outbound access to certain websites or services?**	Proxy server
102.	**1) Bob writes the message 2) Bob encrypts the message with [a]'s [b] key 3) Bob sends the encrypted message to Alice 4) Alice receives the message 5) Using [c]'s [d] key Alice decrypts the message**	Alice public Alice private
103.	**Which technique to control the use of the system's resources is described as: Is the coordinated processing of two or more programs by a system that contains parallel processors.**	Multiprocessing
104.	**Exposure Factor- Your computer that is worth $1800 was mostly destroyed. However, you think you can salvage exactly half of it. Your EF is:**	50%
105.	**Which of the following biometric methods obtain the patterns and colors around a person's pupil?**	Iris scan
106.	**Combine the following using the XOR operation: 10010000000 01110011011**	11100011011
107.	**Which of the following types of authentication is the most common method and also the weakest?**	Password
108.	**What is considered the perfect encryption scheme and is unbreakable?**	b. One-time pad
109.	**What security risk can be associated with interrupt processing?**	b. An interrupted process may assume the priority of the higher level process

110.	**Which type of cipher would you choose if you knew that you were only going to receive a few bytes of data at a time?**	stream cipher
111.	**If the network portion of an IP address is the first octet (10.x.x.x), then the slash notation (also known as CIDR notation) to scan this network is: 10.0.0.0/___**	8
112.	**"All users of Norton anti-viral software will have anti-viral signature files updated weekly. The following procedure is to be followed when updating your anti-virus files every week: ... " is an example of a:**	d. procedure
113.	**What is the act of an unauthorized person intercepting and reading packets that flow across a network?**	Eavesdropping/sniffing
114.	**Because the CPU is the brain of a computer, it and the operating system have multiple layers of self-protection. One mechanism they use is protection rings to separate critical components through boundaries of security controls. Which of the following computer components would be placed in the outermost ring (or layer)?**	b. Applications and programs
115.	**What is a DDOS attack?**	A distributed denial of service attack is typically carried out by a botnet consisting of thousands of infected (zombie) computers which simultaneously send traffic to the targeted site.
116.	**Quantitative**	attempts to assign independent-

		ly objective numeric value to all elements of the risk analysis
117.	**Which of the following protocols does SSH encrypt? (choose all that apply)**	SFTP SCP
118.	**Which of the following is true about an OR statement?**	only one side of the OR statement needs to be true in order for the entire statement to be true
119.	**What is the name of the"big idea" to spread out the message?**	diffusion
120.	**What is "wardriving"?**	Driving around looking for unencrypted wireless access points.
121.	**What technology solution blocks inbound access to internal sites, has anti-virus, and intrusion detection?**	UTM
122.	**The key to protecting assets from the risk of attack is to eliminate or address as many ______ as possible.**	vulnerabilities
123.	**Which of the following is the most effective countermeasure to social engineering?**	Employee education
124.	**Annualized Loss Expectancy is calculated with the following formula:**	ALE = Single Loss Expectancy x Annualized Rate Of Occurrence
125.	**What does Schneier call products that make people feel secure, but don't actually do anything?**	security theatre

126. **According to Bruce Schneier, rare risks are repeated again and again by:**
newspapers

127. **Which one of the following is NOT an effective control against SQL injection attack?**
Client-side input validation

128. **Your corporate firewall has the following rules applied to the incoming interface on the DMZ. If you need to block all web traffic from a malicious source IP address, where would you place an explicit deny statement for that malicious source IP address?**
a) ---- here ------ 10 Permit SRC IP any DST IP 192.168.1.4 SRC PORT any DST PORT 80

129. **One of the first methods of attack was the use of a _______ __________.**
phishing email

130. **Which System Development Life Cylce is more like an assembly line in that it is not very flexible because it doesn't allow you to cyle back through previous steps.**
Waterfall

131. **An IPv6 address is comprised of _____ bits (answer in numeric form).**
128

132. **According to Ralph Langner, in the lab Stuxnet behaved like**
"a lab rat that didn't like the cheese"

133. **In order to list all of the rows from the employee table, what would you enter into the text box that is prompting for the employee ID?**
100' or '1' = '1

134. **In the No Tech Hacking video how did they defeat physical security with junk and stuff (related to the touch bar on the door)?**
they used a hanger and wet towel to unlock a secured door

135. **What protocol is an extension of SSH?**
SFTP